Protection de la vie privée face à l'informatique "made in Belgium"

Boulanger, Marie-Helene; de Terwangne , Cécile; Poullet, Yves

Published in:
Droit de la consommation = Consumentenrecht

Publication date:
1990

Document Version
le PDF de l'éditeur

Protection de la vie privée face à l'informatique made in Belgium

Sommaire

Inhoud

I. Introduction

Le Conseil des Ministres a voté, le 2 février dernier, un avant-projet de loi relative à la protection de la vie privée à l'égard des traitements automatisés d'informations. Le texte, bien que sensiblement modifié et allégé, s'inscrit dans la continuation du dernier projet en date (projet GoI)*(1)*.

Il vise à la transparence de la vie administrative, économique et sociale et cherche à ménager un juste équilibre entre le droit légitime de la société à l'information et le droit au respect de la vie privée de chacun. La démarche adoptée, tout à fait classique dans le paysage européen, consiste à organiser, au fil des dispositions, un régime de protection des informations portant sur un individu, le respect de la vie privée constituant le vecteur de la réglementation. Le raisonnement peut être inversé. Les Italiens ont ainsi, de façon étonnante, préféré dans leur tout récent projet de loi élaborer un régime protecteur basé sur le principe premier du droit à l'information et, partant, de la libre utilisation de l'ordinateur.

Le projet Wathelet est une réponse à l'obligation contractée par notre pays, le 7 mai 1982, lors de la signature de la Convention du Conseil de l'Europe, relative à la protection des données personnelles. La Belgique s'engageait par là à prendre en droit interne les mesures nécessaires en vue de donner effet aux dispositions de la Convention.

Notre Etat, bien qu'ayant figuré parmi les pionniers en matière de protection des données, est à ce jour à la traîne d'une Europe de plus en plus consciencisée par le problème (témoin, la proposition de directive que la Commission européenne a soumis tout récemment au Conseil)*(2)*. Depuis le dépôt de la

première proposition de loi en 1971*(3)*, ni ce texte, ni aucun des multiples autres qui lui feront suite, ne sera adopté définitivement. Si bien que la Belgique se voit aujourd'hui montrée du doigt pour le vide juridique qu'elle présente en la matière et qui laisse les individus dépourvus d'une protection générale et effective face à l'informatique.

Notre propos s'attachera tout d'abord à examiner le champ d'application du projet de loi (II) avant de décrire et d'analyser les principes à la base de la réglementation envisagée (III) et les obligations du ficheur et droits du fiché correspondants (IV). Le statut, le rôle et la compétence de la Commission de la protection de la vie privée feront enfin l'objet d'un développement distinct (V).

II. Champ d'application

1. Ratione materiae

Le champ d'application ratione materiae est particulièrement étendu. Le projet de loi réglemente à la fois le *traitement automatisé* de données et la *tenue d'un fichier manuel* (art. 1 par. 1).
L'exposé des motifs signale à cet égard que la protection s'étend aux fichiers manuels afin d'éviter la prolifération de fichiers manuels « refuges ». L'extension à ce type de fichiers paraît toutefois excessivement large. En effet, la notion de traitement automatisé est définie par le projet de loi comme « tout ensemble d'opérations réalisées *en tout ou en partie* à l'aide de procédés automatisés relatifs à l'enregistrement, la conservation, la modification, l'effacement, la consultation ou la diffusion de données à caractère personnel sous forme de fichier » (art. 1 par. 2).
Une telle disposition permet de couvrir la plupart des fichiers manuels dont la consultation est facilitée par l'utilisation de l'informatique. Il eut dès lors été préférable de prévoir la seule extension de certains prescrits de la loi aux fichiers non automatisés plutôt que de soumettre d'office ceux-ci à l'ensemble des dispositions légales*(4)*.
Le projet s'applique au traitement automatisé et non directement au fichier. La notion de traitement est à comprendre au sens large: outre la phase d'exploitation des informations, sont également à envisager la collecte, la conservation et l'effacement des données. La notion de traitement risque toutefois de poser divers problèmes quant au respect pratique des dispositions légales. Ainsi, lorsqu'une entreprise dispose d'un système d'information caractérisé par différentes applications, on peut se demander si l'entreprise met en œuvre un ou plusieurs traitements.

Aux termes de l'article 1er, le traitement automatisé n'entre dans le champ d'application de la législation que pour autant qu'il contienne des données à caractère personnel et qu'il soit en outre constitué sous forme de fichier.

Tout d'abord, la protection concerne les données *« à caractère personnel»*. Le texte précise, à l'instar de la Convention du Conseil de l'Europe de 1981,

qu'il faut entendre par là les données relatives à une personne physique identifiée ou identifiable (art. 1 par. 5). Les personnes morales sont donc exclues du bénéfice des dispositions du projet de loi*(5)*.

On peut noter ici que la définition de la notion de « données à caractère personnel » adoptée par la Commission européenne dans son projet de directive est particulièrement large, et ce, afin de couvrir l'ensemble des informations qui pourraient être rattachées à un individu. Ainsi, même lorsque l'élément d'identification de la personne concernée est un simple numéro de référence, il faut considérer qu'il s'agit là d'un individu identifiable.

Il doit s'agir ensuite de traitement conservé sous la forme de fichier. Le concept de *fichier* est à distinguer de celui de dossier. Il est défini comme un ensemble de données à caractère personnel constitué et conservé suivant une structure logique devant permettre la consultation (art. 1 par. 3).
L'exposé des motifs précise que « ne constituera donc pas un fichier au sens de la loi une succession de dossiers rangés selon un ordre alphabétique ou numérique ».

Par son caractère artificiel, cette distinction semble difficile à mettre en œuvre dans la pratique. Ainsi, un ensemble de textes enregistrés de façon non structurée sur ordinateur répond à la définition du dossier, alors qu'il est techniquement très simple de lui appliquer un logiciel qui permettrait par exemple de retirer les données nominatives qui s'y trouvent. Le dossier devient-il fichier lorsque les données peuvent en être extraites systématiquement? En outre, le côté flou de la distinction de ces deux notions risque de permettre au détenteur de fichier, s'il le souhaite, de se soustraire en toute légalité aux obligations prévues. Il lui suffit, pour échapper aux dispositions impératives de la loi, de faire sortir l'information d'un fichier et de l'insérer dans un dossier.

Le débat a déjà été ouvert en France, à l'occasion notamment du jugement du Tribunal de Grande Instance de Paris, du 2 mars 1989*(6)*.
Aux yeux du tribunal, les notions de dossier et de fichier peuvent être compatibles, dans la mesure où l'on peut être en présence d'un fichier de dossiers. A l'opposé, commentant l'arrêt, le professeur Gassin estime qu'une « suite de dossiers individuels, si bien organisée soit-elle, ne peut pas être considérée comme l'équivalent d'un fichier, car il y manque ce traitement préalable de documents bruts caractéristiques du fichier qui rend les informations contenues dans le dossier directement et immédiatement utilisables »*(7)*.

Pour le professeur Frayssinet, la distinction absolue entre les deux notions (sur base de quels critères?) est illusoire et à dépasser, la solution étant à trouver dans l'application généralisée des règles de protection à tout ensemble d'informations nominatives utilisées en dehors du cadre strict de la vie privée, sans considération des supports et techniques employés*(8)*.

On le voit, l'unanimité n'est pas acquise... La parole revient en définitive au juge à qui il appartiendra d'interpréter au cas par cas la portée de la distinction.

Sont exclus du bénéfice des dispositions protectrices du projet de loi :
– les traitements gérés par des personnes *physiques* destinés, de par leur nature, à un *usage privé* (art. 3 par. 2). Il peut s'agir tant d'un agenda ou d'un carnet d'adresses que d'un micro-ordinateur personnel;
– les traitements faisant l'objet d'une publicité en vertu d'une disposition légale ou réglementaire ou dont l'intéressé assure ou fait assurer la *publicité* comme, par exemple, l'annuaire téléphonique.

Si la première de ces deux exceptions est tout à fait heureuse, on peut regretter que l'exclusion de la seconde catégorie de traitements de données ne repose pas sur l'application stricte du principe de pertinence. Cela permettrait de ne soustraire aux dispositions protectrices que les traitements qui justifient une telle exclusion en raison de leurs finalités.

2. Ratione personae
Les dispositions du projet de loi s'appliquent à tout détenteur de fichier qu'il s'agisse d'une personne physique, d'une personne morale ou d'une association de fait. Aucune distinction n'est opérée en fonction de l'origine des fichiers : sont dès lors également visés les fichiers du secteur public et les fichiers du secteur privé. Le projet recouvre indifféremment *tout* traitement automatisé de données à caractère personnel.

L'administration de la *Sûreté de l'Etat* et le *Service général du Renseignement* bénéficient d'un régime particulier.
Les dispositions incompatibles avec l'exercice de leurs missions ne leur sont pas applicables (art. 3 par. 3)*(9)*.

Sont, par ailleurs, explicitement exclus du champ d'application, les *institutions de droit international public* dont la Belgique est membre et *l'Institut national des Statistiques* (art. 3 par. 2 b et d). A propos de l'exclusion automatique de ce dernier, une critique semble devoir être émise. Le simple fait que la finalité statistique du traitement des données personnelles implique l'anonymat ne devrait pas suffire à soustraire ces données de la protection mise en place par le projet.

L'arrêt fondamental de la Cour constitutionnelle allemande de Karlsruhe du 15 décembre 1983 est particulièrement éclairant à cet égard*(10)*. La Cour, saisie d'un recours contre la loi de 1983 sur le recensement démographique*(11)*, a reconnu que la totale innocence des données anonymisées n'était pas toujours réelle. Il est en effet parfois possible que des groupes isolés analysés (îlots) trop restreints ou des caractéristiques de classement trop précises conduisent à l'identification d'individus. Partant, les données statistiques peuvent représenter un danger pour la vie privée. L'exclusion du

champ d'application de l'Institut national des Statistiques paraît cependant moins critiquable si l'on sait que ses agents sont soumis au secret statistique.

3. Ratione loci

Le projet de loi s'applique :
– à la tenue *en Belgique* d'un fichier manuel (art. 3 par. 1, 1°);
– au traitement automatisé *directement accessible en Belgique* par des moyens propres au traitement (art. 3 par. 1, 2°).

Une telle définition du champ d'application territorial de la loi belge est de toute évidence aberrante et abusive. Elle permet en effet, à la limite, de soumettre tout traitement à la loi pour autant qu'il s'agisse de traitement accessible par le biais d'un moyen de télécommunication et que le terme « directement » ne soit pas entendu de façon restrictive*(12)*. Un élément de rattachement plus précis est donc absolument nécessaire.

En matière d'information dispensée lors de la collecte de données, le champ d'application est élargi à toute collecte sur le territoire belge en vue d'un traitement, même si le traitement est effectué hors du territoire national (art. 5 par. 1) (infra).

4. Ratione temporis

La période transitoire pour les fichiers existants sera fixée par le Roi (art. 43). Notons que l'expérience des pays ayant adopté une législation en matière de protection de la vie privée, à l'égard des traitements informatisés de données, a montré qu'une période relativement longue était nécessaire pour certains prescrits de la loi, telle la formalité de l'enregistrement des banques de données.

III. Principes de base

1. Principe du respect de la vie privée

L'article 2 du projet de loi consacre le droit fondamental au respect de la vie privée des personnes physiques lors du traitement des données à caractère personnel qui les concernent.
Si un tel principe devait être posé dans un pays où aucun texte interne*(13)* ne fait précisément mention de la vie privée, on peut néanmoins regretter que les termes retenus pour énoncer le droit soient plutôt restrictifs. N'aurait-il pas, en effet, été préférable de parler de respect des libertés publiques et individuelles qui ne soient pas limitées à la seule « vie privée" ? Cela permettrait d'inclure dans les valeurs à protéger, notamment la liberté économique d'obtention de crédit. Lorsque circule, entre organismes de crédit, une liste noire comportant des erreurs, c'est en effet bien plutôt à une telle liberté et non à la vie privée qu'il y a risque d'atteinte*(14)*.

2. Principe de finalité

Second principe essentiel posé par la nouvelle législation - qui est en cela inspirée de la Convention du Conseil de l'Europe, et de l'ensemble des législations étrangères par ailleurs - le principe de finalité et de pertinence est la pierre d'angle de l'équilibre à trouver, entre les intérêts du maître du fichier et le droit au respect de la vie privée de l'individu concerné.
Aux termes de l'article 6 du projet de loi, il ne peut être procédé au traitement de données à caractère personnel qu'en vue de finalités déterminées et légitimes et que pour autant que les données traitées soient pertinentes et non excessives par rapport à ces finalités. Ainsi, tant l'enregistrement et la conservation des données que leur modification, leur consultation et leur diffusion doivent répondre aux objectifs préalablement définis.

S'il est des cas où la détermination des finalités poursuivies est sans équivoque, parce que présente dans un texte légal ou réglementaire (comme pour les données sensibles, v. infra)*(15)*, des doutes peuvent naître parfois quant à la pertinence d'un traitement. C'est aux tribunaux qu'il appartiendra d'évacuer de tels doutes.
Il leur faudra, en outre, être particulièrement attentifs aux tentations de détournement de finalités auxquelles doivent résister les maîtres de fichiers qui, en raison des différentes activités qu'ils poursuivent (ainsi, le cas d'une banque procédant à des opérations d'assurance ou d'une société de grande distribution ayant des participations dans une société de mailing), effectuent divers traitements de données. Ces derniers doivent demeurer distincts les uns des autres et les données recueillies aux fins d'un premier traitement ne peuvent faire l'objet d'un second*(16)*.

En cas de non-respect du principe de finalité et de pertinence, le contrevenant s'expose à de sévères sanctions pénales (lourdes amendes et/ou emprisonnement). Il eût été bon que les auteurs du texte introduisent un critère d'intentionnalité pour déterminer l'imputabilité de la faute, qu'ils ne répriment que la violation sciemment commise. Cela permettrait d'éviter à l'employeur la désagréable expérience - et combien préjudiciable pour l'entreprise - de se voir emprisonner, ensuite du comportement abusif de l'un de ses préposés.

Il peut ici être noté qu'aux Pays-Bas, le législateur a préféré ne pas sanctionner pénalement la violation du principe de finalité mais bien plutôt aggraver la sanction civile.

3. Collecte des informations

Principes
L'article 5 de la Convention du Conseil de l'Europe de 1981 énonce que les données doivent être obtenues de façon loyale et licite. La collecte des données, si elle présente un caractère abusif, peut en effet porter atteinte à la vie privée. La réglementation prévue pallie partiellement à ce risque, en instaurant un devoir d'information à charge du ficheur (art. 4), à l'égard de celui auprès de qui les données à caractère personnel sont recueillies.

Elle n'exige cependant pas - et cela est déplorable - que les données recueillies soient pertinentes, compte tenu des finalités des traitements gérés par les organismes collecteurs.

L'obligation de renseigner le fiché, sanctionnée pénalement (art. 34), porte sur tout ce qui est nécessaire pour l'exercice du droit d'accès de celui-ci.
Il s'agit plus précisément :
– de l'identité et de l'adresse du maître du fichier et, le cas échéant, de son représentant en Belgique;
– de la possibilité d'obtenir des renseignements complémentaires auprès du registre public des traitements automatisés tenu par la Commission pour la protection de la vie privée (infra);
– de l'existence d'un droit d'accès et de rectification (infra).

Il est regrettable que la notification de la finalité de la collecte des informations, également prévue dans une version antérieure du texte apparue lors de l'élaboration du projet, n'ait pas été maintenue dans la version finale.

Le devoir de notification du ficheur n'existe que dans les cas où la collecte est initiale, c'est-à-dire lorsque les données sont directement collectées auprès des intéressés. Lorsque les renseignements enregistrés sont recueillis auprès de tiers, les dispositions de l'article 10, relatives à l'information à donner lors du premier enregistrement s'appliquent (infra).

Les autorités publiques exerçant des compétences de police administrative ou judiciaire sont, bien entendu, dispensées de l'obligation de renseignement (art. 4 par. 2).

Restrictions à la collecte : les données sensibles
La loi réserve un sort particulier aux données sensibles qu'elle énumère en ses articles 7, 8 et 9. Il s'agit de toutes informations nominatives portant sur la race, la vie sexuelle, les opinions politiques, philosophiques ou religieuses et les appartenances syndicales ou mutualistes, de même que des données médicales ou judiciaires concernant un individu.

Ces données ne peuvent faire l'objet d'un traitement qu'en vue de finalités définies au sein d'une loi (v. le régime plus sévère encore des données médicales décrit ci-dessous). Toutefois, des exceptions pourront être admises par le Roi, par la voie d'arrêtés délibérés en Conseil des Ministres, après avis de la Commission de la protection de la vie privée. De plus, les associations sont autorisées à tenir un fichier de leurs membres.

Le projet de directive européenne, en comparaison, va spécialement loin dans sa volonté de protéger les données sensibles (dont l'énumération correspond identiquement aux catégories belges). Ainsi, selon les termes de son texte actuel, ces données ne peuvent faire l'objet d'un traitement automatisé, à moins que la personne intéressée n'y ait donné, par écrit, son consentement

exprès. En outre, les exceptions qui sont admises ne le sont que si un intérêt public important le justifie.

Le fondement sur lequel repose l'instauration d'un régime particulier pour ces catégories de données, n'est plus l'idée de la nécessité de préserver le noyau dur de la vie privée mais bien celle, plus juste, que le traitement de telles données risque d'être source de discrimination vis-à-vis de certaines personnes*(17)*.

Avoir opté pour l'établissement d'une liste « exhaustive » des données sensibles n'est pas la solution la plus heureuse. De nombreux autres pays ont également succombé à cette tentation et il est paradoxal de constater que les listes apparues sont toutes variables. Le caractère sensible ou ordinaire qui s'attache à une information tient en fait au contexte spécifique entourant celle-ci.
Ainsi que l'illustre très justement le professeur Simitis, « on peut, en effet, difficilement soutenir qu'une liste contenant les noms de personnes placées dans des institutions est moins sensible que l'information relative à une extraction de dents » *(18)*.

C'est aussi le contexte, plus précisément la finalité poursuivie, qui est le critère décisif pour justifier le traitement des données sensibles. L'enregistrement de ces données pouvant être légitime au vu de sa finalité, les auteurs du projet de loi auraient pu préférer l'application stricte du principe de pertinence, à l'édiction d'une liste fermée de données interdites. Cela aurait permis d'éviter l'inévitable multiplication des exceptions, tant celles prévues par le texte (pas moins de six exceptions sont envisagées pour les données relatives au passé judiciaire) que celles qui apparaîtraient par suite du recours à la - très lourde - procédure ouverte au Roi.

Données médicales
Il est clair que le respect du secret médical doit recevoir application en matière de traitements automatisés. La loi envisagée pose en conséquence le principe de l'interdiction d'enregistrer des données relatives à l'état de santé, aux examens et aux soins médicaux, de même qu'aux traitements contre l'alcoolisme ou autres intoxications (art. 8 par. 1).

Le traitement de ces données est néanmoins autorisé dans les deux cas suivants :
– avec le *consentement écrit* du patient (art. 8 par. 1, 1°);
– sous la *surveillance et la responsabilité d'un médecin* (art. 8 par. 1, 2°).

Les traitements automatisés de données médicales seront donc normalement gérés par des médecins, les règles de la déontologie leur permettant ou leur imposant de garder le secret.

Les données administratives ou comptables peuvent, quant à elles, être traitées par des établissements de soin, des organismes de sécurité sociale ou de santé publique (art. 8 par. 2).

En ce qui concerne la diffusion d'informations médicales nominatives, le projet reprend le principe général du secret médical et interdit la communication de ces données aux tiers.

La question des données médicales aurait mérité, à elle seule, un examen approfondi et une législation particulière et l'on peut regretter que les auteurs du projet de loi l'aient évacuée en un article. Dans cette matière, en outre, une négocation avec les secteurs concernés eût été hautement souhaitable avant l'élaboration d'un quelconque régime spécifique.

4. Principes relatifs à la gestion

Le texte distingue maître et gestionnaire du fichier. Des obligations spécifiques sont à charge de chacun d'eux.

Le *maître du fichier* est la personne physique ou morale ou l'organisme non doté de la personnalité juridique, compétent pour décider de la finalité du traitement et des catégories de données devant y figurer (art. 1 par 6). Si la finalité du traitement est définie par la loi, le maître du fichier sera la personne déterminée par la loi pour tenir le fichier.
Cette dernière définition est assez ambiguë, évoquant plutôt la notion de gestionnaire du fichier.
Ainsi, le Ministre de l'Emploi et de la Prévoyance sociale est désigné comme le maître du fichier de la banque-carrefour de la sécurité sociale. Or, peut-on voir en lui la personne qui réellement « tient le fichier» ?

Le *gestionnaire du traitement* est la personne physique ou morale ou tout organisme non doté de la personnalité juridique à qui sont confiées l'organisation et la mise en œuvre du traitement (art. 1 par. 7).
Afin de mieux faire comprendre la portée de cette distinction, l'exposé des motifs prend l'exemple du registre central du commerce créé par la loi auprès du Ministère des Classes moyennes et géré en fait par une société privée.
La notion de gestionnaire du traitement paraît toutefois peu opérationnelle, puisqu'elle regroupe à la fois, la personne physique responsable d'assurer le respect de la loi, et la personne morale gérant le système informatisé (service bureau)*(19)*.

Le maître du fichier est soumis à un certain nombre d'obligations dont le respect est contrôlé par la Commission (art. 15). Ces obligations visent, pour une part à assurer un contrôle interne effectif des opérations de traitement de données, pour une autre part à garantir une protection physique des données*(20)*.
Le maître du fichier est ainsi, dans un premier temps, tenu d'établir pour chaque traitement automatisé qu'il contrôle, un état où sont consignés la

nature des données traitées, le but du traitement, les liaisons ou interconnexions, les personnes ayant accès aux données et, enfin, les bénéficiaires de toute transmission des données. Cette exigence est assortie de sanctions pénales. On peut s'interroger sur la réelle opportunité de l'établissement d'un état interne alors que, comme nous le verrons par la suite, une déclaration aux mentions plus complètes, portant sur les mêmes fichiers, doit être également effectuée.

Le détenteur du fichier doit également veiller à l'application régulière des traitements.

Il doit, en outre, informer ses collaborateurs des dispositions à respecter en matière de protection de la vie privée.

Par ailleurs, en ce qui concerne la protection physique des données, le maître du fichier doit s'assurer de la conformité des programmes servant au traitement avec la réglementation.

Il doit, d'autre part, veiller à ce que l'accès au traitement soit limité aux seules personnes qui, en raison de leurs fonctions ou pour les besoins du service, ont directement accès aux informations enregistrées.

Enfin, il est tenu de s'assurer que la communication des données est limitée aux personnes autorisées (tiers ou collaborateurs).

Une ultime obligation pèse sur le maître du fichier. Celle de faire toute diligence pour tenir les données à jour, rectifier ou supprimer les données inexactes, incomplètes ou non pertinentes.

5. Communication des données

Nulle disposition du projet de loi n'établit de manière expresse un régime des communications de données nominatives. Au détour de certaines dispositions, toutefois, les auteurs du texte en font mention. Il ressort de ces allusions que les données traitées ne peuvent être transmises qu'aux personnes autorisées, mentionnées dans l'état interne et dans la déclaration.

Il eût été préférable d'envisager la question, à l'instar du législateur allemand, selon une approche positive. Le principe posé serait alors, non pas l'interdiction de la transmission des données, mais la légalité de celle-ci, pourvu qu'elle soit pertinente dans le chef de celui qui communique les informations et qu'elle soit justifiée par un intérêt légitime du destinataire de ces informations.

L'application logique du principe de pertinence aurait dû permettre d'éviter certaines lourdeurs du texte, telle la création d'un régime spécifique pour la communication des données médicales.

Les interconnexions entre fichiers peuvent être considérées comme une forme particulière de communication des informations aux tiers. Le développement incessant de l'informatique et des technologies de télécommunication et leur mise en relation rendent ce problème plus aigu.
Aussi, il appartiendra au Roi de réglementer ou interdire les interconnexions apparaissant dans les rapports établis par delà les frontières, qui présenteraient des risques pour le droit au respect de la vie privée*(21)*.

Il peut de même restreindre les flux transfrontières de données. Une telle intervention ne peut cependant avoir lieu que dans les limites du respect des conventions internationales auxquelles la Belgique est partie.
Ainsi, notamment, la Convention du Conseil de l'Europe qui, aux termes de son article 12, affirme la libre circulation des données entre pays disposant de législations protectrices équivalentes, vient limiter la possibilité de restrictions, tant aux interconnexions qu'aux simples flux transfrontières d'informations.

IV. Obligations du ficheur, droits du fiché

Les obligations incombant, aux termes de la loi, au maître du fichier, sont à mettre en corrélation avec les droits que le fiché se voit reconnaître, étant donné que le devoir du premier représente la plupart du temps un droit pour le second. C'est donc réunis logiquement dans un même exposé que nous les examinons.

1. Déclaration préalable

Préalablement à sa mise en œuvre, *tout traitement automatisé* doit, sous peine de sanctions pénales (art. 35, 3° et 4°), faire l'objet d'une déclaration auprès de la Commission de la protection de la vie privée (art. 16). La déclaration comportera une douzaine de mentions reprenant les caractéristiques principales du traitement, tels la dénomination, le contenu, le but du traitement, les mesures de sécurité mises en place, les catégories de personnes admises à obtenir les données, ainsi que l'identification des maître et gestionnaire du fichier. Si les données sont destinées à l'étranger, deux mentions supplémentaires, relatives aux catégories de données qui font l'objet de la transmission et à leur pays de destination, doivent être ajoutées.

La formalité de déclaration doit être effectuée par le maître du fichier et renouvelée en cas de modification d'un élément préalablement déclaré. La mise à jour est essentielle et nécessaire pour que la formalité ait un sens, mais il s'agit là d'une opération fastidieuse qui risque bien souvent d'être négligée*(22)*. L'administration de la Sûreté de l'Etat du Ministère de la Justice et le Service général du renseignement et de la sécurité du Ministère de la Défense nationale ne sont pas soumis à cette formalité.

La mise en œuvre du traitement pourra débuter dès que sera effectuée la déclaration. L'accusé de réception adressé par la Commission n'est donc

aucunement suspensif. Il est purement formel et vise à ménager au déclarant une preuve de la réception de son envoi.

Des déclarations réduites ou des exemptions pourront être autorisées par le Roi, sur avis de la Commission de la protection de la vie privée, pour les catégories de traitements qui ne présentent manifestement pas de risques d'atteinte à la vie privée.
Cette possibilité est inspirée du modèle français (normes simplifiées) mais une différence majeure intervient entre les deux systèmes, révélatrice de la différence de poids des organes concernés : si, en France, c'est à la CNIL qu'il appartient d'édicter les normes simplifiées, en Belgique, l'initiative revient au Roi, la Commission n'ayant qu'un pouvoir d'avis.

L'utilisation sensée de cette procédure particulière - sensée dans la mesure où elle ménage un équilibre entre les intérêts contradictoires de l'individu et du ficheur - contribuera à assurer une certaine légèreté de la loi et, partant, son effectivité.

L'accomplissement de la formalité de déclaration est lié au paiement d'une redevance, à l'opposé de l'option prise par la majorité des autres pays européens*(23)*.

Signalons que, lorsque la Commission de la protection de la vie privée estime qu'un *fichier manuel* est susceptible de porter atteinte à la vie privée, elle peut, d'office ou sur requête d'une personne concernée, exiger du maître du fichier en question, soit la même déclaration que celle prévue pour les fichiers automatisés, soit une déclaration réduite (art. 18).

La loi allemande, quant à elle, ne distingue pas selon que le fichier est automatisé ou manuel mais bien plutôt selon qu'il s'agit d'un fichier tenu à des fins internes ou non. Ainsi, les personnes ou entreprises privées procédant au traitement de données personnelles, à des fins purement internes, sont dispensées d'effectuer la formalité de déclaration. Cette solution présente l'avantage de ne pas voir les entreprises privées sombrer dans des excès administratifs et assure par là la praticabilité de la loi*(24)*. Une telle idée était présente dans l'ancien projet Gol, mais à la différence de la loi allemande, la formule belge était critiquable, en ce qu'elle ne préservait pas le droit d'accès de la personne fichée à l'égard de ces traitements et qu'elle n'imposait pas, par ailleurs, la tenue d'un registre interne à l'entreprise.

2. Notification du premier enregistrement

Complémentairement à l'information donnée lors de la collecte (le contenu de l'information donnée est identique) et préalablement à l'exercice effectif du droit d'accès, le texte impose au ficheur de notifier tout premier enregistrement. Lorsqu'une personne est enregistrée pour la première fois dans un traitement de données à caractère personnel, elle doit être immédiatement informée de *l'existence* du fichage (art. 10).

Le maître du fichier se voit toutefois dispensé de cette obligation dans les cas suivants :
– dès lors que la personne concernée a bénéficié d'une information lors de la collecte (infra);
– si le traitement se situe dans une relation contractuelle entre la personne fichée et le maître du fichier;
– et enfin si le traitement se situe dans une relation entre la personne concernée et le maître du fichier, réglée par ou en vertu d'une loi, d'un décret ou d'une ordonnance.

De plus, des mesures collectives d'information ou d'exemption à l'égard de certaines catégories de traitements pourront être prévues par le Roi, sur avis de la Commission de la protection de la vie privée.
Il reste que cette formalité, sanctionnée pénalement (art. 34, 4°), impose de lourdes charges aux détenteurs de fichiers. Or, la communication paraît superflue dans les cas où la personne sait ou peut raisonnablement savoir qu'elle est fichée. La loi hollandaise, dans une optique plus pratique et plus heureuse à notre sens, a adopté ce critère de la « connaissance raisonnable » du fichage pour dispenser le ficheur du devoir de notification. Elle le soustrait en outre également à l'obligation, lorsqu'un intérêt essentiel de la personne concernée s'oppose à une notification écrite.

Il est à noter ensuite qu'un déséquilibre existe entre le secteur privé et le secteur public, ce dernier étant largement dispensé de l'obligation de notification par le biais de la troisième hypothèse d'exclusion envisagée par l'article 10.
Aux termes de celle-ci, en effet, dès lors qu'un traitement se situe dans une relation établie par ou en vertu d'une loi, il n'y a pas lieu de notifier le fichage à la personne concernée. Le projet de loi va ici à l'encontre de la tendance à la transparence de l'administration que l'on observe actuellement dans la majorité des Etats.

3. Droit d'accès, de rectification, de radiation

Droit d'accès
Le droit d'accès permet à quiconque de connaître ce qui est contenu dans un fichier à son sujet. Ce droit fondamental se retouve dans l'ensemble des législations étrangères, ainsi que dans la Convention du Conseil de l'Europe. Le projet de loi belge reconnaît à toute personne justifiant de son identité, le droit d'obtenir communication sous une forme compréhensible des données la concernant dans un traitement automatisé (art. 10 par. 2).

L'exercice du droit d'accès n'est donc subordonné à aucune exigence particulière de motivation. Le texte ne précise pas si la commmunication des données se limite aux données de base enregistrées ou comprend les données de résultat issues du traitement. Il ne spécifie pas plus, par ailleurs, si l'accès s'étend aux données relatives aux circuits internes d'utilisation de l'information et à la transmission des informations à des tiers.

Des sanctions pénales sont prévues en cas de refus de communication ou lorsque des pressions ont été exercées sur la personne concernée, en vue de se faire communiquer par cette dernière les renseignements obtenus par l'exercice de son droit d'accès (art. 35, 1° et 2°). Cette disposition, déjà présente dans le projet Gol, est véritablement originale.

Les conditions et modalités de paiement d'une indemnité destinée à couvrir les seuls frais administratifs peuvent être prévues par le Roi.

Une période de douze mois minimum doit s'écouler entre deux mises en œuvre du droit d'accès. La Commission pour la protection de la vie privée peut toutefois raccourcir ce délai dans des cas exceptionnels (art. 10 par. 3). N'aurait-il pas été préférable, à l'exemple des Pays-Bas et de l'Allemagne*(25)*, de limiter le droit d'accès dans les cas où un intérêt primordial (c'est-à-dire plus important que celui du requérant, en ce compris celui du détenteur du fichier) le justifie ?

Il existe certaines exceptions au principe selon lequel toute personne fichée a directement accès aux données à caractère personnel la concernant. Pour différentes catégories d'informations, le projet a mis en place, selon le modèle français, une procédure d'accès indirect, faisant intervenir un intermédiaire entre le ficheur et le fiché*(26)*.

Les données médicales ne sont ainsi communiquées que par l'intermédiaire d'un médecin désigné par le patient (art. 10 par. 4). Le projet de loi ne s'écarte pas, sur cette question, des règles de la déontologie professionnelle qui traditionnellement refusent le libre accès du patient à son dossier médical.

Le droit d'accès peut également être exercé de manière indirecte, par l'intermédiaire de la Commission de la protection de la vie privée, pour certaines catégories de fichiers publics. Il en est ainsi d'une part, pour les traitements automatisés gérés par les autorités publiques chargées de la recherche, de la constatation ou de la poursuite des infractions et d'autre part, pour les traitements gérés par la Sûreté de l'Etat du Ministère de la Justice, le Service général du renseignement et la sécurité du Ministère de la Défense (art. 10 par. 5 et 12).

La procédure à suivre pour procéder à un accès indirect est la suivante : l'intéressé s'adresse tout d'abord à la Commission, afin que celle-ci exerce pour lui son droit d'accès et de rectification. La Commission procède à toutes les vérifications utiles, ordonne le cas échéant les rectifications ou suppressions qui s'imposent et avertit ensuite simplement l'intéressé qu'il a été procédé aux vérifications nécessaires.

Droit de rectification
Lorsqu'elle connaît les données contenues à son sujet dans un fichier, la personne concernée peut demander gratuitement au maître du fichier la

rectification de toute donnée inexacte la concernant. Elle peut en outre exiger la suppression ou l'interdiction d'utilisation d'une donnée la concernant, qui, au regard de la finalité du traitement, est superflue, incomplète ou non pertinente, ou dont l'enregistrement, la communication ou la conservation sont interdits ou encore qui a été conservée au-delà de la période autorisée.

Si les données sont inexactes, incomplètes ou superflues ou si encore elles ont été communiquées après la période de conservation autorisée, le maître du fichier sera tenu de notifier, soit la rectification, soit la suppression des données aux tiers auxquels ces données ont été transmises, pour autant qu'il connaisse encore ces derniers. Il s'agit là du « droit de suite ».

Le dépôt d'une demande écrite effectuée par la personne concernée désireuse d'exercer son droit de rectification, constitue une formalité préalable à toute procédure judiciaire. Le projet stipule qu'une action ne sera recevable que pour autant que la demande de rectification ait été expressément rejetée ou qu'elle soit demeurée sans suite pendant au moins deux mois.

On peut légitimement s'étonner qu'une telle condition soit énoncée par les auteurs du texte. N'ont-ils pas perçu qu'un ensemble de cas litigieux doivent être tranchés en urgence, que la diffusion de données interdites ou erronées peut conduire à des préjudices immédiats et que l'écoulement obligatoire de deux mois peut faire perdre tout intérêt à l'action (si ce n'est l'éventualité d'un dédommagement) ?

4. Droit de recours

Auprès de la Commission

La Commission se voit attribuer dans le projet de loi des compétences quasi juridictionnelles : elle examine les plaintes relatives à la protection de la vie privée qui lui sont adressées (sans préjudice de toute voie de recours devant les juridictions), assure éventuellement des missions de médiation et dénonce au Procureur du Roi les infractions dont elle a connaissance. L'importance de ses fonctions en cette matière tient d'une part, dans le caractère très souple de la procédure et d'autre part, dans le rôle de l'ombudsman qu'elle sera amenée à jouer.

Les membres de la Commission disposent d'importants pouvoirs d'investigation : ils peuvent requérir le concours d'experts, effectuer des vérifications dans les locaux des établissements concernés et consulter les documents se rapportant aux fichiers.

Lorsque, dans le cadre de lois particulières, des commisssions sectorielles sont créées, chargées entre autres de veiller à la protection des données (ainsi les lois relatives à la banque-carrefour de la sécurité sociale et au registre national des personnes physiques notamment), la Commission de la protection de la vie privée dispose de compétences réduites. Elle jouit d'un droit d'évocation à l'égard des décisions prises par les Comités de surveillance

institués par ces lois particulières. Il ne s'agit pas d'une procédure d'appel : la Commission vérifie uniquement si les principes généraux de la protection de la vie privée ont été respectés.

Auprès du Tribunal

S'il n'a pas été répondu à la demande d'accès ou de rectification des données adressée au maître du fichier, la personne concernée peut former un recours auprès du Président du tribunal de première instance siégeant comme en référé (art. 13). Le projet de loi rend ce dernier compétent pour connaître des règles relatives à l'enregistrement et à la conservation des données.

La demande doit être introduite par requête contradictoire. La compétence du tribunal est déterminée en fonction du domicile du demandeur. L'ordonnance du juge est exécutoire par provision, nonobstant appel ou provision (art. 13 par. 7).

En cas de dommage subi du fait de l'inexactitude des données personnelles ou d'une suppression non autorisée de données, une action ordinaire en responsabilité civile est ouverte à la personne concernée, à l'encontre du maître du fichier.

Lorsqu'apparaît une contestation judiciaire au sujet de données traitées, toute communication de ces données doit indiquer clairement qu'elles sont contestées (art. 14).

D'autre part, le Président du tribunal de première instance, saisi par voie de requête unilatérale, peut ordonner toutes mesures de nature à éviter la dissimulation et la disparition d'éléments de preuve qui peuvent être invoqués dans le cadre de la procédure judiciaire (art. 13 par. 7).

On peut, à notre sens, s'interroger sur l'opportunité de la création de nouvelles procédures dans un système judiciaire déjà suffisamment complexe. Etait-il nécessaire de prévoir, pour les besoins particuliers nés de l'application de cette réglementation, une possibilité de recours spécifique, alors que les procédures existantes (le référé notamment) apportaient une réponse satisfaisante.

V. Commission de la protection de la vie privée

Le projet de loi institue auprès du Ministère de la Justice une commission appelée « Commission de la protection de la vie privée ». Cet organe succède à la Commission consultative de la protection de la vie privée, compétente dans le cadre de la loi du 8 août 1983 organisant un registre national des personnes physiques et de l'arrêté royal n° 141 du 30 décembre 1982 créant une banque de données relative aux membres du personnel du secteur public.

La nouvelle commission se voit reconnaître une assez large autonomie.
On peut voir en elle dorénavant l'autorité indépendante chargée de veiller à la protection de la vie privée à l'égard des traitements de données à caractère personnel, tant dans le cadre du projet de loi générale, que dans le cadre des lois particulières relatives à cette question.

Il est à noter que dans aucune des diverses procédures instaurées par le projet, dans lesquelles l'intervention de la Commission est prévue, l'avis recueilli auprès de cette dernière ne doit être conforme. Cet indice de faiblesse du pouvoir reconnu à cet organe rejoint l'observation déjà formulée à propos de l'autorité compétente pour la prise de « normes simplifiées » concernant la formalité de déclaration (le Roi).

La question des ressources de la Commission est importante dans la mesure où, des moyens d'action mis à sa disposition, dépendra la correcte exécution de la mission qui lui est confiée, de même que la garantie de son indépendance. La Commission se voit attribuer des crédits inscrits au budget du Ministère de la Justice. Le projet de loi pose également que la redevance perçue lors de l'accomplissement de la formalité de déclaration, est versée aux fins d'alimenter un fonds destiné à assurer le fonctionnement de la Commission, formule qui présente l'intérêt de fournir à cette dernière des ressources autonomes mais qui pèseront sur les entreprises.
Un rapport annuel d'activités doit être communiqué aux chambres.

1. Composition

La Commission est composée de membres de droit désignés par les comités de surveillance institués par des lois particulières et de membres désignés sur des listes présentées par le Conseil des Ministres pour un terme de 6 ans, alternativement par la Chambre des Représentants et par le Sénat (art. 23).
La Commission comprend, outre les membres de droit, huit membres effectifs et huit membres suppléants. Le nombre des membres désignés par le Parlement pourra toutefois être augmenté par le Roi, de façon à ce que les membres de droit ne soient jamais majoritaires au sein de la Commission.
Un magistrat choisi parmi les membres effectifs remplit les fonctions de président.

La parité linguistique et l'équilibre socio-économique (?) doivent être respectés.

Les membres sont tenus à un devoir de confidentialité.

2. Compétences

Outre la compétence qui lui est reconnue d'exercer l'accès indirect, examiner les plaintes et assurer un rôle de médiateur, la Commission tient le registre des traitements de données et joue un rôle actif en ce qui concerne l'élaboration des normes ayant trait à la protection de la vie privée.

Tenue du registre des traitements automatisés de données à caractère personnel
La Commission tient un registre public des traitements automatisés, sur base des déclarations qu'elle reçoit des maîtres de fichier (art. 16 et 17).
Le registre comporte, pour chacun des traitements, l'essentiel des mentions reprises dans la déclaration. Il contient également, le cas échéant, des informations sur les fichiers manuels susceptibles de porter atteinte à la vie privée. (art. 18).

Emission d'avis et de recommandations
La Commission peut être amenée à rendre des avis lors de l'élaboration de projets d'arrêtés royaux. A plusieurs reprises, le projet de loi a prévu son intervention dans les procédures d'adoption de mesures complémentaires ou de mesures d'exécution de la nouvelle réglementation*(27)*..

Mais il appartient aussi à cet organe d'émettre des avis ou des recommandations sur toute question relative à l'application des principes fondamentaux de protection de la vie privée dans le cadre des lois existantes (art. 28 par. 1-3).

VI. Conclusion

Lorsqu'il a annoncé que, pleinement conscient du besoin de plus en plus pressant d'une protection des données qui se faisait sentir dans notre pays, il s'attacherait à apporter une réponse législative au problème, le Ministre de la Justice a déclaré qu'il était préférable à ses yeux d'adopter rapidement un texte même imparfait, plutôt que de laisser les individus sans protection dans l'attente d'une loi totalement satisfaisante.

Dans cet ordre de choses, si le texte qu'il nous propose aujourd'hui présente des qualités certaines, il n'en est pas pour autant idéal et quelques remarques finales peuvent ici être formulées.

Tout d'abord, l'accent mis sur la protection de la vie privée risque de laisser dans l'ombre la protection plus large des libertés individuelles, sur laquelle il serait bon de focaliser l'intérêt.

Ensuite, une référence plus fréquente et une application plus stricte du principe de finalité conduirait, à la fois, à plus de simplicité, plus de légèreté et plus de souplesse de la législation. Dans le même ordre d'idée, l'expérience étrangère a démontré qu'il valait mieux opter pour une loi cadre dans laquelle sont énoncés des principes généraux (relatifs à la qualité des données, l'information du fiché,...) plutôt que prétendre traiter exhaustivement la question. En marge de la loi cadre, des législations sectorielles fleuriraient, au terme d'une négociation avec les différents acteurs concernés.

En tant que garante d'une protection effective des données, il ne faut pas craindre de confier à la Commission des compétences solides avec, à la clef, des moyens humains et financiers suffisants. Cet organe devant être avant tout un outil de dialogue, il faut éviter, en outre, de monopoliser son énergie pour l'accomplissement de lourdes tâches administratives.

Enfin, on peut s'étonner que le texte de la loi ne distingue pas entre fichiers du secteur public et fichiers du secteur privé, types si fondamentalement différents qu'ils devraient obéir à des règles spécifiques. Ainsi, les banques de données du secteur public devraient répondre à des principes tels que la création en vertu de la loi, la clarté des missions données à chaque système d'information étatique et la transparence de leur fonctionnement, alors que les traitements de données effectués dans le secteur privé doivent trouver leur légitimité dans la relation contractuelle entre le ficheur et le fiché.

Quoi qu'il en soit, la parole revient dorénavant au Parlement qui devra être attentif à l'évolution de la situation sur la scène européenne, afin d'éviter un hiatus entre la législation belge et la directive communautaire.

M.H. BOULANGER et C. de TERWANGNE,
sous la direction du Professeur Y. POULLET

Samenvatting

BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER BETREFFENDE INFORMATICA, MADE IN BELGIUM

1. De Raad van Ministers heeft op 2 februari 1990 een voorontwerp van wet ter bescherming van de persoonlijke levenssfeer in het domein van de geautomatiseerde gegevensbestanden goedgekeurd. Het ontwerp Wathelet sluit aan bij de ondertekening in 1982 van de Conventie van de Raad van Europa betreffende de bescherming van persoonlijke gegevens, en zou een belangrijk hiaat in onze achtergebleven wetgeving moeten opvullen.

2. Het toepassingsgebied « ratione materiae » is zeer ruim en heeft zowel betrekking op manuele als op geautomatiseerde gegevensbestanden. Het wetsontwerp beoogt echter niet de bestanden als dusdanig maar wel de geautomatiseerde behandeling ervan, in de ruime zin van het woord. Verder is vereist dat het gaat om gegevens met een persoonlijk karakter, die deel uitmaken van een bestand. De auteur wijst op het kunstmatig onderscheid tussen dossier en bestand, en evalueert de uitzonderingen die in het wetsontwerp voorzien zijn.
Het toepassingsgebied « ratione personae » betreft zowel natuurlijke personen als rechtspersonen, en zowel de privé-sektor als de openbare sektor.

Verder heeft de auteur het over het toepassingsgebied « ratione loci » en « ratione temporis ».

3. Bij de behandeling van de basisprincipes staat de auteur stil bij het begrip « persoonlijke levenssfeer » en bij de finaliteit en pertinentie als hoeksteen voor de beoordeling van de wederzijdse belangen van de « geficheerde » en de meester van het bestand. Na een kommentaar bij de voorziene strafrechtelijke sancties worden de principes en beperkingen betreffende het verzamelen van gegevens behandeld, waarna de auteur nader ingaat op de medische gegevens.
Wat het beheer van de gegevensbestanden betreft, maakt de wet een onderscheid tussen de meester en de beheerder, elk met hun eigen verplichtingen. Het wetsontwerp voorziet geen uitdrukkelijke regeling betreffende de mededeling van gegevens, hetgeen door de auteur wordt betreurd, verwijzend naar de Duitse wetgeving.

4. De verplichtingen van de meester of beheerder van een bestand en van de geficheerde worden gezamenlijk behandeld omdat verplichtingen van de ene meestal neerkomen op rechten van de andere. Voordat een geautomatiseerd gegevensbestand operationeel wordt, moet dit het voorwerp uitmaken van een gedetailleerde verklaring bij de Commissie voor de bescherming van de persoonlijke levenssfeer. Na advies van die Commissie zullen via een KB beperkte verklaringen of vrijstellingen kunnen toegestaan worden voor bepaalde niet gevoelige behandelingscategoriëen. Ter aanvulling van de informatie die bij het verzamelen van de gegevens aan een geregistreerde wordt verstrekt moet de meester van het bestand elke eerste registratie melden en moet de geficheerde onmiddellijk van het bestaan van een bestand (met behandeling van persoonlijke gegevens) geïnformeerd worden. Hierop bestaan echter uitzonderingen.
De geficheerde beschikt over een recht van toegang, rechtzetting en schrapping, die door de auteur in detail worden toegelicht en beoordeeld.

5. Na de behandeling van de verhaalmiddelen van de geficheerde (voor de Commissie en de rechtbank) weidt de auteur uit over de samenstelling en bevoegdheden van de Commissie en besluit, verwijzend naar verklaringen van de Minister van Justitie, volgens dewelke een snelle goedkeuring van een zelfs onvolmaakt wetsontwerp te verkiezen is boven een nijpend gebrek aan bescherming, dat het ontwerp toch voor een aantal verbeteringen vatbaar is, o.m. wat het finaliteitsprincipe betreft, de bevoegdheden van de Commissie en het onderscheid tussen publieke en privé-gegevensbestanden.

(1) Documents parlementaires, Ch., *1330, Sess. parl. 1984-1985.*

(2) Sur le plan international, la protection de la vie privée à l'égard des traitements de données à caractère personnel a retenu l'attention des Nations Unies, du Conseil de l'O.C.D.E. (lignes directrices du 23 septembre 1980 régissant la protection de la

vie privée et les flux transfrontières de données à caractère personnel), du Conseil de l'Europe et de la Communauté économique européenne.
Plus particulièrement, la Convention du Conseil de l'Europe relative à la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, ouverte à la signature des Etats membres le 28 janvier 1981 et signée par la Belgique, est entrée en vigueur le 1er octobre 1985 et lie actuellement 8 pays (l'Autriche, la France, la République Fédérale d'Allemagne, le Luxembourg, la Norvège, l'Espagne, la Suède et le Royaume-Uni).
En matière de droit communautaire, le Parlement européen a montré son intérêt pour cette question, en souhaitant l'édiction de règles communautaires, par l'adoption de trois résolutions, le 8 mai 1979 et le 9 mars 1982 (invitant les Etats membres à ratifier la Convention du Conseil de l'Europe) et le 12 avril 1989 (portant adoption d'une déclaration des droits et libertés fondamentaux).
La Commission a, elle, adopté une communication au Conseil sur la protection des données personnelles et la sécurité de l'information, comportant notamment le texte de projet d'une directive d'harmonisation des législations des Etats membres concernant la protection des individus face au traitement des données personnelles.

Législations étrangères :

Autriche : Loi fédérale n°565 sur la protection des données personnelles du 18 octobre 1978 (réglementant les secteurs public et privé et prévoyant en principe une autorisation administrative pour les flux transfrontières de données), amendée en 1987.

Danemark : Loi n°293 du 8 juin 1978 sur les fichiers privés et loi n°294 du 8 juin 1978 sur les fichiers des autorités publiques, amendées le 1er avril 1988.

France : Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Hongrie : Loi du 27 janvier 1981 sur la protection des données et la liberté d'information.

Irlande : Loi sur la protection des données de 1988.

Islande : Loi n°63/1981 du 25 mai 1981 relative à l'enregistrement systématique de données personnelles, renouvelée et légèrement amendée le 1er janvier 1986.

Luxembourg : Loi du 31 mars 1979 réglementant l'utilisation de données nominatives dans les traitements informatiques.

Norvège : Loi n°48 du 9 juin 1978 sur les fichiers de données personnelles, amendée le 12 juin 1987.

Pays-Bas : Loi du 13 juillet 1988 sur l'enregistrement de données personnelles.

République Fédérale d'Allemagne : Loi fédérale du 27 janvier 1977 sur la protection des données d'identification personnelles, amendée en 1987 et différentes lois sur la protection des données dans les Länder (en voie d'amendement).

Royaume-Uni : Loi sur la protection des données du 12 juillet 1984.

Suède : Loi n°289 du 11 mai 1973 sur les données à caractère personnel, amendée par les lois n°334 du 1er juillet 1979 et n°446 du 1er juillet 1982.

Suisse : Loi fédérale du 23 mars 1988 sur la protection des données et plusieurs lois cantonales et un certain nombre de réglementations municipales.

(3) Documents parlementaires, Sénat, *706, Sess. parl. 1970-1971.*

(4) POULLET, Y., « Informatique et libertés : un débat en quête de solutions », La Semaine Informatique, *1990, n°184, pp. 32-44. Voir l'art. 45 al 1 de la loi française.*

(5) Compar. à ce sujet la loi française n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (cf. LUCAS, A., Le droit de l'informatique, *Presses Universitaires de France, Paris, 1987, n° 95) et l'interprétation de la Commission Nationale Informatique et Libertés à ce sujet (cf HUET, J., MAISL, H.,* Droit de l'informatique et des télécommunications, *LITEC, 1989, n°215).*
L'exclusion des personnes morales se retrouve dans l'ensemble des législations des pays de la CEE à l'exception des seules lois luxembourgeoise et danoise.

(6) Cahiers Lamy du droit de l'informatique, *juin 1989 (d), p. 26.*

(7) GASSIN, R., « Commentaire du jugement du tribunal correctionnel de Paris, du 2 mars 1989 ou, de la distinction des fichiers nominatifs et des dossiers individuels », in Cahiers Lamy du droit de l'informatique, *août 1989 (E), pp. 3 et s.*

(8) FRAYSSINET, J., « Contre l'excessive distinction entre fichier et dossier », Expertises, *1990, n°124, pp. 16-22.*

(9) La loi considère ainsi comme non applicables les dispositions suivantes : art. 4 et 5 relatifs à l'information à fournir lors de la collecte de données, art. 7 à 9 ayant trait aux données sensibles, art. 10 et 11 portant sur les droits d'accès et de rectification, art. 13 règlant la compétence du tribunal de 1ère instance, art. 14 imposant de marquer d'un indice de doute les données communiquées faisant l'objet d'une contestation, art. 16 à 19 concernant la formalité de déclaration auprès de la Commission, enfin art. 28 par. 4 qui donne à la Commission compétence en matière d'examen des plaintes relatives à la protection de la vie privée.

(10) Bundesverfassungsgericht, 15 décembre 1983, B VerfGE 65, 1, 47.

(11) BURKERT, H., « Le jugement du tribunal constitutionnel fédéral allemand sur le recensement démographique et ses conséquences », Droit de l'informatique, *1985, n°4, p. 8 et svts ; CNIL, 5e, Rapport d'activité, La Documentation française, Paris, pp. 176 et svts.*

(12) POULLET, Y., op. cit., p. 41.

(13) Bien que non inscrit dans notre Constitution, le principe du respect de la vie privée est déjà affirmé à l'article 12 de la Déclaration universelle des droits de l'homme et à l'article 8 de la Convention européenne des droits de l'homme et des libertés fondamentales (directement applicable en droit belge).

(14) Sur l'impasse à laquelle mène l'approche, « vie privée » et l'intérêt d'une approche fondée sur la protection des libertés, lire RIGAUX, F., La protection de la personne et de la vie privée, *UCL, Faculté de droit, Louvain-La-Neuve et POULLET, Y., « Le fondement du droit à la protection des données nominatives : propriété ou liberté », Colloque de Montréal, Novembre 1989, inédit.*

(15) Le projet va ici moins loin toutefois que la jurisprudence allemande qui pose que la finalité de tout traitement du secteur public doit être précisée au sein d'une loi. V. Bundesverfassungsgericht, 15 décembre 1983, BVerfGE 65, 1, 47.

(16) POULLET, Y., op. cit., p. 42.

(17) POULLET, Y., op. cit., p. 41.

(18) SIMITIS, S., Les données sensibles en quête d'un régime juridique, Conférence sur les problèmes législatifs de la protection des données, Athènes, 1987, inédit, p. 6.

(19) POULLET, Y., op. cit., p. 42.

(20) BARET, J., « Persoonsgegevens en privacybescherming : een nieuwe wet in de maak. Beschermingstechnieken », Studiedag interdisciplinair Centrum voor recht en informatica, *10 mai 1990, Louvain, inédit, p. 4.*

(21) Les modalités doivent en être fixées par arrêté royal délibéré en Conseil des Ministres, après avis de la Commission de la protection de la vie privée.

(22) L'exemple français du registre de la CNIL est éloquent. Ce dernier comporte des adresses dépassées ou le nom de responsables entretemps remplacés.

(23) Seuls l'Irlande et le Royaume-Uni imposent le paiement d'une somme d'argent.

(24) C'est en outre la solution adoptée dans le projet de directive européenne, qui dispense de la déclaration les traitements de données qui ne sont pas destinées à être communiquées.

(25) Voir l'article 30 de la loi néerlandaise du 13 juillet 1988 relative à l'enregistrement des données personnelles (WPR) et l'article 13 par. 3 de la loi fédérale allemande pour la protection des données (BDSG).

(26) Voir loi française, art. 39 et 40.

(27) Art. 7, 9 par. 2 et 5, 10 par. 1, 12, 16 par. 7, 20 et 21.